Wieder verspekuliert

Super-GAU für Intel: Weitere Spectre-Lücken im Anflug

Neue Lücken und noch mehr Patches – „Spectre Next Generation“ steht direkt vor der Tür. Acht neue Sicherheitslücken in Intel-Prozessoren haben Forscher bereits gefunden, wie Informationen belegen, die c’t exklusiv vorliegen.

Von Jürgen Schmidt

Spectre und Meltdown erschütterten die IT-Welt in ihren Grundfesten: Forscher wiesen nach, dass das Design aller modernen Prozessoren ein prinzipielles Problem aufweist, das ihre Sicherheit gefährdet [1]. Dann gab es Patches und die Welt schien wieder in Ordnung. Zwar warnten einige Experten, dass da noch mehr folgen könnte. Doch es blieb die Hoffnung, dass die Hersteller das Problem mit ein paar Sicherheits-Updates in den Griff bekommen.

Diese Hoffnung können wir begraben. Ganze acht neue Sicherheitslücken in Intel-CPUs haben mehrere Forscher-Teams dem Hersteller bereits gemeldet, die aktuell noch geheimgehalten werden. Alle acht sind im Kern auf dasselbe Design-Problem zurückzuführen, das der Kasten „Meltdown und Spectre für Dummies“ näher erläutert – sie sind sozusagen Spectre Next Generation.

c’t liegen exklusive Informationen zu Spectre NG vor, die wir auf mehreren Wegen verifizieren konnten, sodass wir an deren Echtheit keine Zweifel mehr hegen. Technische Details werden wir jedoch noch nicht veröffentlichen, solange noch eine Chance besteht, dass die Hersteller ihre Sicherheits-Updates vor dem Bekanntwerden der Lücken fertig bekommen. Wir werden unsere Informationen jedoch nutzen, um kommende Veröffentlichungen von Patches und Hintergrundinformationen journalistisch zu begleiten.

Acht neue Lücken

Jede der acht Lücken hat eine eigene Nummer im Verzeichnis aller Sicherheitslücken bekommen (Common Vulnerability Enumerator, CVE) und jede erfordert eigene Patches – wahrscheinlich bekommen sie auch alle eigene Namen. Bis dahin nennen wir sie gemeinsam die Spectre-NG-Lücken, um sie von den bisher bekannten Problemen abzugrenzen.

Konkrete Informationen liegen uns bisher nur zu Intels Prozessoren und deren Patch-Plänen vor. Es gibt jedoch erste Hinweise, dass zumindest einzelne ARM-CPUs ebenfalls anfällig sind. Weitergehende Recherchen dazu, ob und in welchem Maß etwa die eng verwandte AMD-Prozessorarchitektur für die einzelnen Spectre-NG-Lücken anfällig ist, laufen bereits.

An einigen Spectre-NG-Patches arbeitet Intel bereits selbst; andere werden in Zusammenarbeit mit den Betriebssystemherstellern erarbeitet. Wann die ersten Spectre-NG-Patches kommen, ist bislang nicht klar. Unseren Informationen zufolge plant Intel zwei Patch-Wellen: Eine erste soll bereits im Mai anrollen; eine zweite ist derzeit für August geplant.

Für mindestens einen der Spectre-NG-Patches steht schon ein konkreter Termin im Raum: Googles Project Zero hat erneut eine der Lücken gefunden und im Mai läuft die Frist ab, die sie dem Hersteller typischerweise vor einer Veröffentlichung der Details zu einer Lücke einräumen. Googles Elite-Hacker sind recht kompromisslos, was solche Termine angeht und veröffentlichten nach deren Ablauf schon öfter Informationen zu Schwachstellen, für die der Hersteller noch keine Patches fertig hatte. Bei einer zweiten Lücke rechnet Intel selbst damit, dass Informationen jederzeit an die Öffentlichkeit kommen könnten. Für diese beiden Lücken sollten Patches also eher früher als später erscheinen.

Auch Microsoft bereitet sich offensichtlich schon auf CPU-Patches vor: Ursprünglich wurde für Microcode-Updates gegen Spectre auf BIOS-Updates verwiesen, nun erscheinen sie doch in Form von (optionalen) Windows-Updates. Die PC-Hersteller brauchen wohl schlichtweg zu lange für BIOS-Updates. Microsoft lobt zudem in einem Bug-Bounty-Programm für Spectre-Lücken bis zu 250.000 US-Dollar Prämie aus. Die Linux-Kernel-Entwickler tüfteln ebenfalls kontinuierlich an Härtungsmaßnahmen gegen Spectre-Attacken.

Gefährlicher als Spectre

Vier der Spectre-NG-Sicherheitslücken stuft Intel selbst mit einem „hohen Risiko“ ein; die Gefahr der anderen vier ist lediglich als mittel bewertet. Nach unseren eigenen Nachforschungen sind Risiken und Angriffsszenarien bei Spectre-NG ähnlich einzustufen wie bei Spectre – mit einer Ausnahme.

Eine der Spectre-NG-Lücken vereinfacht Angriffe über Systemgrenzen hinweg so stark, dass wir das Bedrohungspotential deutlich höher einschätzen als bei Spectre. Konkret könnte ein Angreifer seinen Exploit-Code in einer virtuellen Maschine (VM) starten und von dort aus das Wirts-System attackieren – also etwa den Server eines Cloud-Hosters. Oder er greift die auf dem gleichen Server laufenden VMs anderer Kunden an. Passwörter und geheime Schlüssel für sichere Datenübertragung sind sehr begehrte Ziele auf Cloud-Systemen und durch diese Lücke akut gefährdet. Intels Software Guard Extensions (SGX), die auf den Schutz sensibler Daten auf Cloud-Servern abzielen, sind übrigens ebenfalls nicht Spectre-sicher [2].

Angriffe auf andere VMs oder das Wirts-System waren zwar prinzipiell auch schon mit Spectre möglich; doch die reale Umsetzung erforderte so viel Vorwissen, dass sie extrem schwierig war. Die erwähnte Spectre-NG-Lücke lässt sich jedoch recht einfach auch für Angriffe über Systemgrenzen hinweg ausnutzen; die Gefahr erhält damit eine neue Qualität. Besonders betroffen sind folglich Anbieter von Cloud-Diensten wie Amazon oder Cloudflare und natürlich deren Kunden.

Die konkrete Gefahr für Privatleute und Firmen-PCs ist hingegen eher gering, weil es dort in aller Regel andere, einfacher auszunutzende Schwachstellen gibt. Trotzdem sollte man sie ernst nehmen und die anstehenden Spectre-NG-Updates nach deren Erscheinen zügig einspielen.

Allerdings deutet einiges darauf hin, dass das alles nicht ganz reibungslos funktionieren wird. Bereits bei der Bereitstellung der Spectre-Updates gab es mehrere Pannen, trotz mehr als sechs Monaten Vorlauf. Obendrein reduzieren manche der Patches die Performance und einige Firmen verweigern BIOS-Updates für wenige Jahre alte Computer. Das alles wird mit Spectre NG eher schlimmer als besser werden.

Viele der c't-Investigativ-Recherchen sind nur möglich dank Informationen, die Leser und Hinweisgeber direkt oder anonym an uns übermitteln.

Wenn Sie selbst Kenntnis von einem Missstand haben, von dem die Öffentlichkeit erfahren sollte, können Sie uns einen anonymen Hinweis oder brisantes Material zukommen lassen. Nutzen Sie dafür bitte unseren anonymen und sicheren Briefkasten.

https://heise.de/investigativ

Kein Loch, sondern Schweizer Käse

Insgesamt zeigen die Spectre-NG-Lücken, dass Spectre und Meltdown keine einmaligen Ausrutscher waren. Es handelt sich eben nicht um ein simples Loch, das man mit ein paar Flicken nachhaltig stopfen könnte. Es verdichtet sich vielmehr das Bild einer Art Schweizer Käse: Für jedes abgedichtete Loch tauchen zwei andere auf. Das ist die Folge davon, dass bei der Prozessorentwicklung der letzten zwanzig Jahre Sicherheitserwägungen immer nur die zweite Geige gespielt haben.

Ein Ende der Patches für Hardware-Probleme der Spectre-Kategorie ist jedenfalls nicht in Sicht. Doch eine niemals endende Patch-Flut ist keine akzeptable Lösung. Man kann sich nicht schulterzuckend damit abfinden, dass die zentrale Kernkomponente unserer gesamten IT-Infrastruktur ein grundsätzliches Sicherheitsproblem aufweist, das immer wieder zu Problemen führen wird.

Natürlich muss Intel die aktuellen Lücken erst einmal möglichst schnell verarzten – und das passiert auch. Doch

Bisherige CPU-Sicherheitslücken Meltdown und Spectre

Google-Name	Kurzbezeichnung	CVE-Nummer
Spectre Variante 1	Bounds Check Bypass	CVE-2017-5753
Spectre Variante 2	Branch Target Injection (BTI)	CVE-2017-5715
Meltdown (GPZ V3)	Rogue Data Cache Load	CVE-2017-5754
GPZ steht für Google Project Zero, Spectre V1 und V2 werden auch GPZ V1 und GPZ V2 genannt		

gleichzeitig gilt es, das CPU-Design grundsätzlich zu überdenken. Werner Haas von der deutschen Firma Cyberus Technology und einer der Mitentdecker von Spectre/Meltdown, hält es für durchaus möglich, High-Performance-Prozessoren mit einem soliden Sicherheits-Design auszustatten. Dazu müssten jedoch die Sicherheitsaspekte von Beginn an in der Architektur berücksichtigt werden. Der ebenfalls an der Spectre-Enthüllung beteiligte Paul Kocher hat zusätzliche, besonders gesicherte CPU-Kerne ins Gespräch gebracht. Und mit Methoden wie Threat Modelling kann man heute risikobehaftete Techniken durchaus auch so umsetzen, dass die Sicherheit beherrschbar bleibt.

Intel hat Anfang Januar das Versprechen „Sicherheit zuerst“ gegeben. Jetzt muss das Unternehmen für mehr Transparenz sorgen und beispielsweise Risikoanalysen zu potenziellen Schwachstellen veröffentlichen. Bisher handelt Intel eher nach dem Motto „Wir sind die Experten, wir machen das schon richtig“ – etwa bei Techniken wie der Intel Management Engine und den Software Guard Extensions. Damit sollten wir uns nicht mehr abspeisen lassen, wenn es um zentrale Komponenten unserer IT-Infrastruktur geht.

(ju@ct.de) c't

Literatur

[1] Olivia von Westernhagen, Verspekuliert, Meltdown&Spectre-Angriffe im Detail, c't 3/2018, S. 62
[2] Dr. Johannes Götzfried, RAM-Schranke, RAM-Verschlüsselung bei AMD und Intel, c't 10/2018, S. 174

Meltdown und Spectre für Dummies

Für eine vereinfachte Erklärung der Meltdown- und Spectre-Angriffe muss man eigentlich nur zwei grundsätzliche Dinge über moderne CPUs wissen. Erstens: Da Hauptspeicher viel langsamer ist als die CPU, verwendet man superschnelle Zwischenspeicher, die Caches. Die Speicherverwaltung sorgt dafür, dass darin möglichst immer schon die Werte stehen, die die CPU als nächstes braucht. Ein einmal in den Cache geladener Wert bleibt auch vorerst dort liegen, weil er oft noch weitere Male benötigt wird.

Zweitens: Moderne CPUs führen Befehle nicht immer in der Reihenfolge aus, wie sie im Code stehen. Um vorhandene Ressourcen optimal zu nutzen, versuchen sie, sämtliche parallel arbeitende Funktionseinheiten kontinuierlich zu beschäftigen. Dazu sortiert die CPU manche Befehle um (Out of Order Execution) oder führt Befehle aus, von denen noch gar nicht klar ist, ob sie wirklich an die Reihe kommen (Speculative Execution).

Dazu spekuliert die CPU bei einer Verzweigung im Code-Pfad, welcher Weg wahrscheinlich genommen wird (Branch Prediction). Für diese spekulativ ausgeführten Befehle gelten sonst übliche Sicherheitsregeln zunächst nicht. So führt die CPU etwa einen lesenden Speicherzugriff erst einmal aus und prüft erst im Nachhinein, ob das auch erlaubt war. Falls nicht, macht sie bereits ausgeführte Arbeitsschritte wieder rückgängig. Obwohl das Zeit kostet, gewinnt die CPU insgesamt, weil sie häufig richtig spekuliert. Das Sicherheitskonzept dafür lautet vereinfacht: „Ich mach erst mal und räum dann später auf.“

So viel zum Grundwissen, jetzt zum Angriff. Nehmen wir an, dass auf Ihrem PC Ihre supergeheime Glückszahl „7“ an einer bekannten Stelle im Speicher steht. Sie führen das von mir geschriebene, vermeintlich nützliche Programm trojaner.exe aus. Das versucht heimlich, Ihre Glückszahl auszulesen. Weil trojaner.exe jedoch die nötigen Zugriffsrechte fehlen, verhindert die CPU dies und löst stattdessen einen Zugriffsfehler aus. Das muss ein Computer sicherstellen können, sonst taugt er nicht für sicherheitsrelevante Aufgaben.

Nach diesem gescheiterten Angriff schicke ich Ihnen jedoch das noch viel nützlichere Programm meltdown.exe, das an dieser Sicherheitsbarriere vorbeikommt. Es sorgt erstens dafür, dass die CPU den eigentlich verbotenen Lesezugriff auf Ihre Glückszahl spekulativ ausführt, also mit reduzierten Sicherheitsvorkehrungen. Zweitens trickst es das Aufräumen aus.

Letzteres funktioniert so: meltdown.exe legt als erstes für alle möglichen Werte der Glückszahl eine Schublade an. Diese werden dann explizit „kaltgestellt“; das bedeutet, sie befinden sich nur im langsamen Hauptspeicher, nicht im Cache.

Durch das spekulative Ausführen bekommt das Programm ganz kurz Zugriff auf den Geheimwert 7. Bevor es diesen dauerhaft speichern kann, schlägt das CPU-Aufräumkommando zu und macht alles rückgängig, was meltdown.exe mit diesem Wert angestellt hat – aber nur fast: Im kurzen Zeitfenster der Vorabausführung schreibt meltdown.exe in die siebte Schublade. Und damit landet die siebte Schublade im Cache – sie ist also „heiß“, und zwar als einzige.

Der Rest ist einfach: meltdown.exe liest den Inhalt aller Schubladen aus und misst dabei die Zugriffszeiten. Dabei fällt die siebte Schublade aus der Reihe: Der Zugriff erfolgt hier sehr viel schneller, weil sich der Inhalt bereits im Cache befindet. Die heiße Schublade verrät also meltdown.exe Ihre geheime Glückszahl 7 – und damit auch mir, dem Angreifer. Experten sprechen von einer Timing-Attacke beziehungsweise einem Seitenkanalangriff über den Cache.

Spectre funktioniert ähnlich, ist allerdings in den Details deutlich komplizierter. So liest spectre.exe die geheime Information nicht selbst aus, sondern manipuliert die spekulative Ausführung anderer Programme oder sogar des Betriebssystems, um den gesuchten Geheimwert letztlich ebenfalls mit dem Seitenkanalangriff über den Cache zu ermitteln. Noch schlimmer wirkt Spectre, wenn es in einer virtuellen Maschine (VM) auf einem Cloud-Server läuft, zusammen mit weiteren VMs anderer Nutzer. Denn dort teilen sich alle VMs dieselbe (Intel-)CPU. Dann kann spectre.exe andere VMs oder sogar das Host-System angreifen.